ROGUE AP DETECTION

Background of the Invention

The present invention is directed to the field of security measures for wireless LAN technology. In a wireless local area network (or WLAN) a wireless client seeks to connect to the network in order to exchange data. There are three states in connecting to the network as specified by the IEEE 802.11 specification for WLANs:

1. Unauthenticated and Unassociated
2. Authenticated and Unassociated
3. Authenticated and Associated.

Authentication is the process of verifying the credentials of a client desiring to join a WLAN. Association is the process of associating a client with a given Access Point (AP) in the WLAN. IEEE 802.11 defines two types of authentication methods - Open Key System Authentication and Shared Key Authentication. A successful completion of the association and authentication phases allows a WLAN node successful entry into the WLAN subsystem.

The IEEE 802.11b standard attempts to provide "privacy of a wire" using an optional encryption scheme called "Wired Equivalent Privacy" (or WEP) in which a data frame or "payload" is run through an encryption algorithm, the output of which replaces the original payload. With "open key authentication" the entire authentication process is done in clear text. This means since the entire process is performed without encryption, a client can associate to the AP with the wrong WEP key or no WEP key. But as soon as the client tries to send or receive data it is denied access for not having the correct key to process the packet. With "shared key authentication" there is a challenge text packet that is sent within the authentication process. If

the client has the wrong key or no key it will fail this portion of the authentication process and will not be allowed to associate to the AP.

This choice (open or shared key) is manually set on each device (AP and client). There should be a match in the method chosen by the client and the AP for the association to succeed. The default value is for open authentication.

The entire process can be broken down into three phases:

1) Probe Phase

When a client is initialized it first sends a "probe request" packet out on all the channels. The APs that hear this packet will then send a "probe response" packet back to the station. This probe response packet contains information such as SSID (Service Set Identifier), which the client utilizes to determine which AP to continue the association process with.

2) Authentication Phase

After the client determines which AP to continue association process with, it begin the authentication phase based upon the probe response packet. This phase can be performed in either open or shared key mode. The client and the access point both have to be set-up to the same authentication scheme for this phase to be performed properly.

OPEN AUTHENTICATION SCHEME: The client sends an authentication request to the AP. The AP then processes this request and determines (based on the configured policies) whether or not to allow the client to proceed with the association phase. The AP sends an authentication response packet back to the client. Based upon the type of response (pass or fail) from the AP, the client will either continue or discontinue the association process.

SHARED KEY AUTHENTICATION: The client sends an authentication request to the AP. The AP processes this request, generates and sends a challenge text packet to the client. The client is then required to encrypt the packet utilizing its already-configured WEP key and send the packet back up to the AP. The AP then determines if it can decipher the packet correctly. Based upon this test, the AP will send either a pass or fail in the authentication response packet to the client that determines if the client is allowed to continue the association phase or not.

3) Association Phase

When the client successfully completes the authentication phase (for example, receives a successful authentication response packet from the AP), it proceeds to the association phase. The client sends an association request packet to the AP. The AP analyses the information in this packet and if it passes, the AP adds the client to its association table. It then sends an association response packet to the client, which completes the association phase.

One of the primary drawbacks with the IEEE 802.11 shared key authentication scheme is that there is no mutual authentication between the client and the AP. Only the client authenticates to the access point but the access point does not authenticate to the client. This opens up the doors for denial of service attacks via rogue APs in the WLAN. Such attacks redirect legitimate users having their data open to plaintext or other attacks by associating with APs that are masquerading as members of the WLAN sub system. Mutual authentication between the client and the AP that requires both sides to prove their legitimacy within a reasonable time is critical to detecting and isolating rogue access points.

The existing IEEE 802.11b standard is severely handicapped with its availability for only the current open and shared key authentication scheme that is essentially non-extensible. WLAN customers will demand and expect to receive flexibility in next generation security solutions. Some of these requirements include the addition of new 802.11 authentication methods. The authentication methods need to remain independent of the underlying 802.11 hardware to the greatest extent possible since hard-coding any authentication methods makes it difficult to respond to security vulnerabilities that are constantly discovered and that require quick rollout of fixes. Extensibility is required in order to support Public Key Infrastructure (PKI) and certificate schemes

There is no standard mechanism that allows a network administrator to control access to and from a LAN segment based on the authenticated state of a port user. Simple network connectivity affords anonymous access to enterprise data and the global internet. As 802 LANs are deployed in more accessible areas, there is an increasing need to authenticate and authorize basic network access. The proposed project will provide common interoperable solutions using standards based authentication and authorization infrastructures already supporting schemes such as dial up access.

Summary of the Invention

In view of the difficulties and drawbacks associated with the previous systems, there is a need for an authentication method that remains independent of the underlying hardware.

There is also a need for an authentication method that enables responsiveness to security vulnerabilities and a quick rollout of fixes.

There is also a need for a system and method that provides extensibility in order to support PKI and certificate schemes.

There is also a need for a system and method that decreases hardware cost and complexity.

There is also a need for a system and method that enables customers to choose their own security solution.

There is also a need for a system and method that permits the implementation of the latest, most sophisticated authentication and key management techniques with modest hardware.

There is also a need for a system and method that enables rapid development response to security issues.

These needs and others are satisfied by the method and implementation for network authentication of the present invention as disclosed herein. The invention is realized in a method of detecting a rogue access point comprising the steps of directing a message from a supplicant to a network through an access point and receiving a network response message by the supplicant from the access point. A step of determining whether the access point is one of a valid network access point and a rogue access point is included based on whether the received network response message is respectively in conformity and nonconformity with predetermined expectations.

As will be realized, the invention is capable of other and different embodiments and its several details are capable of modifications in various respects, all without departing from the invention. Accordingly, the drawing and description are to be regarded as illustrative and not restrictive.

Brief Description of the Drawings

Figs. 1 and 2 illustrate a network authentication arrangement in accordance with the present invention.

Figs. 3 through 7 depict steps in the authentication process in accordance with the present invention.

Detailed Description of the Invention

The present invention contemplates a flexible security framework to support enhancements that would overcome the disadvantages of previous systems. Cisco, Microsoft and several other vendors have endorsed the role of the developing IEEE 802.1X standard as the preferred framework for edge security and are actively participating in the standardization efforts to foster interoperable implementations. The IEEE 802.1X Working Group is chartered with the goal of providing an interoperable security framework for port based access control that resides in the upper layers (for example, above the MAC layer). The primary philosophy for the port based access control layer is to enable the plug-in of new authentication schemes and key management methods without changing switches, NICs, Access Points, and so on. Another goal is to also leverage the main CPU resources for cryptographic calculations. This security philosophy is intended to provide end users and customers with decreased hardware cost and complexity, to enable customers to choose their own security solution, to permit the implementation of the latest, most sophisticated authentication and key management techniques with modest hardware, and to enable rapid development response to security issues.

When a host connects to the LAN port on a 802.1X switch and Access Point, the authenticity of the host is determined by the switch port according to the protocol specified by 802.1X, before the services offered by the switch are made available on that port. Until the authentication is complete, only EAPOL (see below) frames are allowed to be sent and received on that port. Once the host authentication is successful, the port switches traffic as a regular port. As an example, when a Windows 2000 PC is hooked on to a LAN switch port, and when a user logs in, the switch sends a message requesting the PC to identify itself. When the PC responds back with an identity frame, the switch makes use of the service of an authentication server to verify the credentials of the user. If the authentication server informs that the user is authentic, then the switch opens its port for providing the network services of the switch.

As used herein in describing the present invention and as shown in Fig. 1, a "port" is a single point of attachment to the LAN infrastructure - for example, ports of MAC Bridges. A "Port Access Entity" (PAE) operates the algorithms and protocols associated with the authentication mechanisms for a given port of the system. An "authenticator PAE" 10 is an access point that wishes to enforce authentication before allowing access to services that are accessible via that port. The authenticator PAE 10 is responsible for communication with the supplicant, and for submitting the information received from the supplicant to a suitable authentication server in order for the credentials to be checked and for the consequent authorization state to be determined. The functionality of authenticator PAEs is independent of the actual authentication method. It merely acts as a pass-through for the authentication exchange, for example, a switch port. The "supplicant PAE" 12 is a PAE that wishes to access the services accessible via the authenticator. The supplicant PAE is responsible for responding to requests from the authenticator 10 for information that will establish its credentials, for

example, an end-user PC, e.g. a Windows 2000 PC connected to the LAN switch port. An "authentication server" 14 verifies the credentials of the supplicant 12. It indicates in response whether or not the supplicant 12 is authorized to access the authenticator's services. It basically provides the authentication service for the authenticator PAE 10 that acts as a client, for example, a RADIUS server.

The IEEE 802.1X standard makes authentication more generic rather than enforcing a specific mechanism on the devices. 802.1X makes use of Extensible Authentication Protocol (EAP) for communication information. The 802.1X standard defines a standard for encapsulating the Extensible Authentication Protocol messages to that they can be handled directly by a LAN MAC service. This encapsulated form of an EAP frame is known as an Extensible Authentication Protocol Over LAN (EAPOL) frame and is defined in the standard. Alternatively, with Extensible Authentication Protocol Over Wireless (EAPOW), the EAPOL messages described earlier are encapsulated over 802.11 wireless frames. The packet exchange for an IEEE 802.1X conversation using EAP is highlighted in Fig. 2. These messages are a sub set of the 802.1X for 802.11 implementation described below since there is no WEP key required for wired 802.1X networks.

The EAP protocol described above was originally designed to provide an extensible method for a "point-to-point protocol" (PPP) server to authenticate its clients and possibly for the client to authenticate the server. The protocol describes an extensible packet exchange to allow the passing of authentication information between the client and the PPP server. Normally PPP servers rely on a centralized authentication server to validate the clients on their behalf. One of the more popular types of servers is a RADIUS server. Extensions to the RADIUS protocol have been contemplated to allow the passing of the EAP packets between the authentication server and

the PPP server. In this case the PPP server is just a relay agent with the authentication conversation happening between the client and the RADIUS server. The RADIUS server informs the PPP server of the result of the authentication and whether to allow the client to access the network.

It has been contemplated to adapt EAP to WLANs using Public Key Infrastructure (PKI) with EAP-TLS as the authentication method. However, PKI schemes are very compute-intensive on the client systems, require careful planning and design of the overall architecture, and the overall solution costs may be prohibitive for typical enterprises. The only other defined authentication method EAP-MD5 was inadequate, as it does not support mutual authentication between the client and the authentication server.

The EAP protocol was designed so that any type of network access server could use it to validate its clients. In the case of a wireless access point the link to its radio client is not a PPP link but a WLAN. The IEEE 802.1X EAP over LAN (EAPOL) specification defines a method for encapsulating EAP packets in either Ethernet or token ring packets such that they may be transmitted over a LAN. The 802.11 specification also allows for data traffic between the client and access point to be encrypted using a WEP encryption key. In early implementations, the access point would have a single key, which had to be programmed into each client radio and all traffic in the wireless cell would be encrypted with the single key.

The present invention includes a newly-developed protocol called the "light extensible authentication protocol" (EAP-Cisco Wireless or "LEAP") authentication type. With the present invention, using EAP authentication, the client and RADIUS server have a shared secret, usually a username and password combination. The RADIUS can pass enough information to the access point such that the client and access point may independently derive an encryption key that is

unique for this client-access point pair. EAP-Cisco Wireless offers the following benefits: requires minimal support from the client CPU while offering mutual authentication; support for embedded systems, such as printers; support for host machines running operating systems that did not have the support for native EAP or routines to allow the use of the PKI authentication; and support for all popular operating systems such as Windows 95, Windows 98, Windows NT, Windows 2000, Windows Millennium, Windows CE, Linux and Mac OS 9.X.

In a preferred embodiment of the present invention, as shown in the figures, the present invention satisfies the critical security requirements of large enterprises while offering hassle-free WLAN deployment. The illustrated design preferably includes the following WLAN security components: Cisco Secure Access Control Server version 2.6, running on Windows NT Server or Windows 2000 Server, used for AAA and EAP RADIUS services; Cisco Aironet Series access points supporting software version 11.0 or greater for 802.1x EAP authenticator support; and Cisco Aironet client adapters with firmware 4.10 or greater that provide support for integrated network logon and EAP-Cisco Wireless authentication. This exemplary embodiment has been observed to demonstrate the following benefits to enterprise customers: Centralized Authentication and Key distribution; mutual authentication between the WLAN client and the AAA server; broad operating system support; immunity to several WLAN security attacks including rogue AP; and an extensible framework to enable uniform enterprise perimeter security

As shown in Fig. 3, the EAP-Cisco Wireless implementation in accordance with the preferred embodiment comprises three components described as follows. A EAP-Cisco Wireless supplicant 22 is provided, available as a driver update for Windows 95, 98, NT, 2000, Windows Millennium, WinCE, Linus and Mac OS 9.X. This EAP-Cisco Wireless supplicant 22 is preferably a piece of client software and firmware that resides on the host PC with the WLAN

adapter. The EAP-Cisco Wireless supplicant 22 can be set-up to either have the username and password stored in the WLAN NIC card or to have it be manually entered via a network logon process. An 802.1X for 802.11 authenticator 20 is provided to be available as a software update for Cisco 340 series and newer access points. A EAP-Cisco Wireless authentication server 24 is preferably a RADIUS Server that implements EAP-Cisco Wireless authentication, preferably the Cisco Secure Access Control Server (ACS) Version 2.6. The entire authentication and key distribution process is accomplished in three phases, Start, Authenticate and Finish as illustrated in Fig. 3.

Figs. 4 through 7 summarize the different packet exchanges for each phase between the EAP-Cisco Wireless supplicant 22, the access point authenticator 20, and the EAP-Cisco Wireless -RADIUS server 24. Fig. 4 shows an 802.1X over 802.11 exchange using the EAP-Cisco Wireless authentication protocol.

The start phase of EAP-Cisco Wireless Authentication is shown in Fig. 4. In the start phase the following packets are exchanged between the entities. The EAPOW-Start (or EAPOL-Start in 802.1X for Wired networks) is used to start the authentication process and is directed by the client/supplicant 22 to the AP/authenticator 20, in accordance with 802.1X. The EAP-Request/Identity is used by the AP/Authenticator 20 to request the client's/supplicant's identity, in accordance with the message definition in RFC 2284. The EAP-Response/Identity is used by the client/supplicant 22 to deliver the identifying user name and password to the AP/Authenticator 20, in accordance with the definition in RFC 2284.

The Authenticate Phase of EAP-Cisco Wireless Authentication is shown in Fig. 5. The authenticate sequence can vary based on the mutual authentication method chosen between the client 22 and the authentication server 24. For example, with the present EAP-Cisco Wireless

authentication, the sequence of messages occurs as described in the preferred embodiment of Fig. 5. In the preferred embodiment as shown in Fig. 6, the EAP-Response/Identity message from the client/supplicant 22 is forwarded to the RADIUS server 24 by the AP 20 in the form of a RADIUS-Access-Request with EAP extensions, in which EAP is encapsulated in the RADIUS protocol. The RADIUS server 24 then responds back to the access-request with a RADIUS-challenge, which then gets responded to by the client 22, in accordance with the RADIUS protocol described in RFC 2138. The present EAP-Cisco Wireless authentication is a mutual authentication method with the access point 20 in the middle acting solely as a transport vehicle. For example, the access point 20 in the authenticate phase moves the contents of the packets from EAP to RADIUS and vice versa. In this way, no logon functions are performed through the AP, thereby precluding network access to rogue APs.

Alternately, the present invention can support other message types, such as Transport Level Security (TLS) as described in RFC2286 to transfer certificates in a PKI implementation, in which EAP-TLS described in RFC2716 messages would be used. Other such message types can also be used without departing from the invention.

The finish phase of the present EAP-Cisco Wireless Authentication is shown in Fig. 7. If the user is discovered to be invalid, the RADIUS server 24 sends a RADIUS deny packet with an embedded EAP fail. If the user is discovered to be valid, the server 24 sends a RADIUS-Access-Accept packet with an EAP success attribute. The RADIUS-Access-Accept message also contains the MS-MPPE-Send-Key attribute defined by RFC2548 to the access point 20. The key needs to be sent to the access point 20 in order for it to obtain the session key that the client 22 will be using to talk with it. Both the client 22 and the RADIUS server 24 who are using the EAP-Cisco Wireless authentication derive the session key from the user's password. The IEEE

802.11's encryption may be based on a 40/64-bit or 104/128-bit key. The key derivation routines provide a key longer than needed. When the access point 20 receives the key from the RADIUS server 24 (via the MS-MPPE-Send-Key attribute) it sends an EAPOL-KEY message to the client 22 supplying the key length and key index to use. The key value (or actual WEP key) is not sent since the client 22 has already derived it on its own using preloaded algorithms and reference data corresponding to those preloaded into the authentication server. The packet is encrypted using the full-length derived key. The access point 20 also sends an EAPOL-KEY message supplying the length, key index and value of the multicast/broadcast key. This packet is also encrypted using the full-length derived session unicast key. This completes the entire mutual authentication and key derivation and transfer between the EAP-Cisco Wireless Authentication Server 24 and the EAP-Cisco Wireless Supplicant 22. Thus, the intermediary access points 20 only pass the encrypted packets, and do not "share the secret," i.e. do not possess the means to decrypt the packets. In this way, the clients of the WLAN have become invulnerable to rogue AP attacks.

The present invention is particularly useful for detecting rogue access points that may seek to access the network. During the start phase of authentication, the client/supplicant 22 directs a packet to the network, e.g. the server 24, through the AP/authenticator 20. A network response packet is received by the client/supplicant 22 from the network, through the AP/authenticator 20. In order to detect a rogue access point, the client/supplicant 22 performs a routine of determining whether the access point 20 is a valid network access point or a rogue access point. This determination is based on whether the received network response packet is in conformity or nonconformity with predetermined expectations. The "predetermined

expectations" can include the "shared secret" information disclosed hereinabove or any other standard applied for determining conformity.

In the preferred embodiment, a valid network access point 20 conforms with expectations if it forwards data traffic from the network conforming with IEEE 802.1X standards. If the forwarded data traffic is determined by the client/supplicant 22 to not conform, the access point is determined to be a rogue access point. Further, in another preferred embodiment, a valid network access point 20 is determined to conform with predetermined expectations if the mutual authentication disclosed hereinabove is successful. Non-conformity is determined by the failure of the mutual authentication. After issuing a challenge from the server 24 to the client 22, the client 22 issues a counter-challenge back to the server 24. Mutual authentication fails at the counter-challenge step if the username and password of the access point are not found in the server's database. At that point, the access point is identified as a rogue AP.

In the event the access point 20 is determined to be a valid network access point, the access point 20 and supplicant 22 are authenticated to the network. If the access point is determined to be a rogue access point, it is reported as such to the network. In one aspect, the rogue access point is reported to the network by the client 22 through a valid network access point 20, at a later time after the client 22 has contacted a valid AP and authenticated to the network.

The EAP-Cisco Wireless Authentication and Key distribution can be deployed in a large campus. EAP-Cisco Wireless supplicant or client software is preferably supported by a variety of operating systems, including Windows 95, Windows 98, Windows NT 4.0, Windows 2000, Windows Millennium, WinCE 3.0, Mac OS 9.x, and any other type of platform that may be

commonly used. The client authentication can be set-up to work in the default open/shared-key modes defined by the standards or in EAP-Cisco Wireless mode.

As described hereinabove, the present disclosure identifies the important requirements for large-scale enterprise WLAN solutions and summarizes the limitations of first generation WLAN security solutions and the types of security attacks they are susceptible to. The present disclosure outlines the architecture of next generation WLAN solutions that mitigate these concerns. The present disclosure also demonstrates the extensibility built into this framework through support for several mutual authentication schemes, thus offering investment protection as well as a future-proof design. Using WLAN solutions in accordance with the present invention, enterprises can now confidently deploy and benefit from large-scale wireless networks without compromising network security.

As described hereinabove, the present invention therefore solves many problems associated with previous type methods and implementations. However, it will be appreciated that various changes in the details, materials and arrangements of parts which have been herein described and illustrated in order to explain the nature of the invention may be made by those skilled in the are within the principle and scope of the invention will be expressed in the appended claims.